a) der Schwere und Dauer des Verstoßes;

b) ob durch den Verstoß schwerwiegende Mängel in Bezug auf Verfahren, Managementsysteme, Risikomanagement und interne Kontrollen des kritischen IKT-Drittdienstleisters offengelegt wurden;

c) ob Wirtschaftskriminalität erleichtert oder herbeigeführt wurde oder auf andere Weise mit dem Verstoß in Verbindung steht;

d) ob der Verstoß vorsätzlich oder fahrlässig begangen wurde;

e) ob die Aussetzung oder Kündigung der vertraglichen Vereinbarungen ungeachtet der Bemühungen des Finanzunternehmens um Vermeidung von Störungen bei der Erbringung seiner Dienstleistungen ein Risiko für die Fortführung der Geschäftstätigkeit des Finanzunternehmens mit sich bringt;

f) gegebenenfalls der gemäß Absatz 5 auf freiwilliger Basis ersuchten Stellungnahme der gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden, die für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig sind.

Die zuständigen Behörden gewähren Finanzunternehmen den erforderlichen Zeitraum, damit sie die vertraglichen Vereinbarungen mit kritischen IKT-Drittdienstleistern anpassen können, um nachteilige Auswirkungen auf ihre digitale operationale Resilienz zu vermeiden und ihnen die Anwendung der in Artikel 28 genannten Ausstiegsstrategien und Übergangspläne zu ermöglichen.

(9) Die Entscheidung gemäß Absatz 6 wird den in Artikel 32 Absatz 4 Buchstaben a, b und c genannten Mitgliedern des Überwachungsforums und dem JON mitgeteilt.

Die von den Entscheidungen gemäß Absatz 6 betroffenen kritischen IKT-Drittdienstleister arbeiten uneingeschränkt mit den betroffenen Finanzunternehmen zusammen, insbesondere im Zusammenhang mit dem Verfahren zur Aussetzung oder Kündigung ihrer vertraglichen Vereinbarungen.

(10) Die zuständigen Behörden unterrichten die federführende Überwachungsbehörde regelmäßig über die Herangehensweisen und Maßnahmen, die sie bei ihren Aufsichtsaufgaben in Bezug auf Finanzunternehmen gewählt haben, sowie über die von den Finanzunternehmen geschlossenen vertraglichen Vereinbarungen, wenn kritische IKT-Drittdienstleister Empfehlungen, die von der federführenden Überwachungsbehörde an sie gerichtet wurden, teilweise oder vollständig nicht befolgt haben.

(11) Die federführende Überwachungsbehörde kann auf Verlangen die zur Anleitung der zuständigen Behörden abgegebenen Empfehlungen näher erläutern.

Artikel 43

Überwachungsgebühren

(1) Die federführende Überwachungsbehörde erhebt gemäß dem in Absatz 2 genannten delegierten Rechtsakt von kritischen IKT-Drittdienstleistern Gebühren, die die notwendigen Ausgaben der federführenden Überwachungsbehörde für die Durchführung von Überwachungsaufgaben gemäß dieser Verordnung vollständig decken, einschließlich der Erstattung aller Kosten, die durch die Arbeit des in Artikel 40 genannten gemeinsamen Untersuchungsteams entstehen können, sowie der Kosten für die Beratung durch die in Artikel 32 Absatz 4 Unterabsatz 2 genannten unabhängigen Sachverständigen in Angelegenheiten, die in den Aufgabenbereich der direkten Überwachungstätigkeiten fallen.

Die Höhe einer Gebühr, die einem kritischen IKT-Drittdienstleister in Rechnung gestellt wird, deckt alle Kosten ab, die aufgrund der Erfüllung der in diesem Abschnitt festgelegten Aufgaben anfallen, und steht in einem angemessenen Verhältnis zu dessen Umsatz.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 57 einen delegierten Rechtsakt zur Ergänzung dieser Verordnung durch Festlegung der Höhe der Gebühren und der Art und Weise ihrer Entrichtung bis zum 17. Juli 2024 zu erlassen.

Artikel 44

Internationale Zusammenarbeit

(1) Unbeschadet des Artikels 36 können die EBA, die ESMA und die EIOPA im Einklang mit Artikel 33 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1095/2010 bzw. (EU) Nr. 1094/2010 Verwaltungsvereinbarungen mit Regulierungs- und Überwachungsbehörden von Drittländern schließen, um die internationale Zusammenarbeit in Bezug auf das IKT-Drittparteienrisiko in verschiedenen Finanzsektoren zu fördern, insbesondere durch die Entwicklung bewährter Verfahren für die Überprüfung von IKT-Risikomanagementverfahren und -kontrollen, Abmilderungsmaßnahmen und Reaktionsmaßnahmen bei Vorfällen.

(2) Die ESA legen dem Europäischen Parlament, dem Rat und der Kommission über den Gemeinsamen Ausschuss alle fünf Jahre einen gemeinsamen vertraulichen Bericht vor, in dem die Ergebnisse einschlägiger Gespräche mit den in Absatz 1 genannten Behörden von Drittländern zusammengefasst werden, wobei der Schwerpunkt auf der Entwicklung des IKT-Drittparteienrisikos und den Auswirkungen auf die Finanzstabilität, die Marktintegrität, den Anlegerschutz und das Funktionieren des Binnenmarkts liegt.

KAPITEL VI

Vereinbarungen über den Austausch von Informationen

Artikel 45

Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen

(1) Finanzunternehmen können Informationen und Erkenntnisse über Cyberbedrohungen untereinander austauschen, einschließlich Indikatoren für Beeinträchtigungen, Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, soweit dieser Austausch von Informationen und Erkenntnissen

a) darauf abzielt, die digitale operationale Resilienz von Finanzunternehmen zu stärken, insbesondere indem für Cyberbedrohungen sensibilisiert, die Verbreitung von Cyberbedrohungen eingeschränkt oder verhindert wird und die Verteidigungsfähigkeiten, Techniken zur Erkennung von Bedrohungen, Abmilderungsstrategien oder Phasen der Reaktion und Wiederherstellung unterstützt werden;

b) innerhalb vertrauenswürdiger Gemeinschaften von Finanzunternehmen erfolgt;

c) durch Vereinbarungen über den Austausch von Informationen umgesetzt wird, die den potenziell sensiblen Charakter der ausgetauschten Informationen schützen und Verhaltensregeln unterliegen, in deren Rahmen die Wahrung des Geschäftsgeheimnisses, der Schutz personenbezogener Daten im Einklang mit der Verordnung (EU) 2016/679 und Leitlinien für die Wettbewerbspolitik vollumfänglich befolgt werden.

(2) Für die Zwecke von Absatz 1 Buchstabe c werden in den Vereinbarungen über den Austausch von Informationen die Voraussetzungen für die Teilnahme und gegebenenfalls die Einzelheiten zur Einbindung staatlicher Behörden und der Eigenschaft, in der diese in die Vereinbarungen über den Austausch von Informationen eingebunden werden können, zur Einbindung von IKT-Drittdienstleistern sowie zu operativen Aspekten, einschließlich der Nutzung spezieller IT-Plattformen, festgelegt.

(3) Finanzunternehmen teilen zuständigen Behörden ihre Einbindung in die in Absatz 1 genannten Vereinbarungen über den Austausch von Informationen mit, sobald ihre Mitwirkung bestätigt wurde bzw. endet und diese Beendigung in Kraft ist.

KAPITEL VII

Zuständige Behörden

Artikel 46

Zuständige Behörden

Unbeschadet der Bestimmungen über den Überwachungsrahmen für kritische IKT-Drittdienstleister gemäß Kapitel V Abschnitt II dieser Verordnung wird die Einhaltung dieser Verordnung durch die folgenden zuständigen Behörden im Einklang mit den durch die jeweiligen Rechtsakte übertragenen Befugnissen sichergestellt:

a) bei Kreditinstituten sowie bei nach der Richtlinie 2013/36/EU ausgenommenen Instituten durch die gemäß Artikel 4 der genannten Richtlinie benannte zuständige Behörde und bei gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuften Kreditinstituten durch die EZB im Einklang mit den mittels der genannten Verordnung übertragenen Befugnissen und Aufgaben;

b) bei Zahlungsinstituten, einschließlich der nach der Richtlinie (EU) 2015/2366 ausgenommenen Zahlungsinstitute, bei E-Geld-Instituten, einschließlich der nach der Richtlinie 2009/110/EG ausgenommenen Institute, und bei den in Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 genannten Kontoinformationsdienstleistern durch die gemäß Artikel 22 der Richtlinie (EU) 2015/2366 benannte zuständige Behörde;

c) bei Wertpapierfirmen durch die gemäß Artikel 4 der Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates ([38]) benannte zuständige Behörde;

d) bei gemäß der Verordnung über Märkte von Krypto-Werten zugelassenen Anbietern von Krypto-Dienstleistungen und Emittenten von an Vermögenswerte geknüpften Tokens durch die gemäß der entsprechenden Bestimmung der genannten Verordnung benannte zuständige Behörde;

e) bei Zentralverwahrern durch die gemäß Artikel 11 der Verordnung (EU) Nr. 909/2014 benannte zuständige Behörde;

f) bei zentralen Gegenparteien durch die gemäß Artikel 22 der Verordnung (EU) Nr. 648/2012 benannte zuständige Behörde;

g) bei Handelsplätzen und Datenbereitstellungsdiensten durch die gemäß Artikel 67 der Richtlinie 2014/65/EU benannte zuständige Behörde und die zuständige Behörde im Sinne von Artikel 2 Absatz 1 Nummer 18 der Verordnung (EU) Nr. 600/2014;

h) bei Transaktionsregistern durch die gemäß Artikel 22 der Verordnung (EU) Nr. 648/2012 benannte zuständige Behörde;

i) bei Verwaltern alternativer Investmentfonds durch die gemäß Artikel 44 der Richtlinie 2011/61/EU benannte zuständige Behörde;

j) bei Verwaltungsgesellschaften durch die gemäß Artikel 97 der Richtlinie 2009/65/EG benannte zuständige Behörde;

k) bei Versicherungs- und Rückversicherungsunternehmen durch die gemäß Artikel 30 der Richtlinie 2009/138/EG benannte zuständige Behörde;

l) bei Versicherungsvermittlern, Rückversicherungsvermittlern und Versicherungsvermittlern in Nebentätigkeit durch die gemäß Artikel 12 der Richtlinie (EU) 2016/97 benannte zuständige Behörde;

m) bei Einrichtungen der betrieblichen Altersversorgung durch die gemäß Artikel 47 der Richtlinie (EU) 2016/2341 benannte zuständige Behörde;

n) bei Ratingagenturen durch die gemäß Artikel 21 der Verordnung (EG) Nr. 1060/2009 benannte zuständige Behörde;

o) bei Administratoren kritischer Referenzwerte durch die gemäß den Artikeln 40 und 41 der Verordnung (EU) 2016/1011 benannte zuständige Behörde;

([38]) Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Beaufsichtigung von Wertpapierfirmen und zur Änderung der Richtlinien 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU und 2014/65/EU (ABl. L 314 vom 5.12.2019, S. 64).

p) bei Schwarmfinanzierungsdienstleistern durch die gemäß Artikel 29 der Verordnung (EU) 2020/1503 benannte zuständige Behörde;

q) bei Verbriefungsregistern durch die gemäß Artikel 10 und Artikel 14 Absatz 1 der Verordnung (EU) 2017/2402 benannte zuständige Behörde.

Artikel 47

Zusammenarbeit mit den durch die Richtlinie (EU) 2022/2555 geschaffenen Strukturen und Behörden

(1) Um die Zusammenarbeit zu fördern und den aufsichtlichen Austausch zwischen den gemäß dieser Verordnung benannten zuständigen Behörden und der durch Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe zu ermöglichen, können sich die ESA und die zuständigen Behörden bei Angelegenheiten, die ihre Aufsichtstätigkeiten in Bezug auf Finanzunternehmen betreffen, an den Tätigkeiten der Kooperationsgruppe beteiligen. Die ESA und die zuständigen Behörden können verlangen, zur Teilnahme an den Tätigkeiten der Kooperationsgruppe in Angelegenheiten im Zusammenhang mit den wesentlichen oder wichtigen, von der Richtlinie (EU) 2022/2555 erfassten Unternehmen, die ebenfalls gemäß Artikel 31 der vorliegenden Verordnung als kritische IKT-Drittdienstleister eingestuft wurden, eingeladen zu werden.

(2) Die zuständigen Behörden können sich gegebenenfalls an die zentralen Anlaufstellen und die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten CSIRT wenden und mit ihnen Informationen austauschen.

(3) Die zuständigen Behörden können gegebenenfalls die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden um einschlägige fachliche Beratung und Unterstützung ersuchen und Kooperationsvereinbarungen schließen, um die Einrichtung wirksamer und schneller Koordinierungsmechanismen zu ermöglichen.

(4) In den in Absatz 3 genannten Vereinbarungen können unter anderem Verfahren für die Koordinierung der Aufsichts- bzw. Überwachungstätigkeiten in Bezug auf wesentliche oder wichtige, von der Richtlinie (EU) 2022/2555 erfasste Unternehmen, die gemäß Artikel 31 der vorliegenden Verordnung als kritische IKT-Drittdienstleister eingestuft wurden, festgelegt werden, wozu die Durchführung von Untersuchungen und Vor-Ort-Inspektionen im Einklang mit dem nationalen Recht sowie Mechanismen für den Informationsaustausch zwischen den gemäß der vorliegenden Verordnung zuständigen Behörden und den gemäß der genannten Richtlinie benannten oder eingerichteten Behörden, einschließlich des Zugangs zu den von den letztgenannten Behörden angeforderten Informationen, gehören.

Artikel 48

Zusammenarbeit der Behörden

(1) Die zuständigen Behörden arbeiten untereinander und gegebenenfalls mit der federführenden Überwachungsbehörde eng zusammen.

(2) Die zuständigen Behörden und die federführende Überwachungsbehörde tauschen zeitnah alle relevanten Informationen über kritische IKT-Drittdienstleister aus, die sie benötigen, um ihre jeweiligen Aufgaben gemäß dieser Verordnung wahrnehmen zu können, insbesondere in Bezug auf die ermittelten Risiken, die Herangehensweisen und die Maßnahmen, die im Rahmen der Überwachungsaufgaben der federführenden Überwachungsbehörde ergriffen wurden.

Artikel 49

Sektorübergreifende Übungen, Kommunikation und Zusammenarbeit im Finanzbereich

(1) Die ESA können über den Gemeinsamen Ausschuss und in Zusammenarbeit mit — je nach Sachlage — den zuständigen Behörden, den in Artikel 3 der Richtlinie 2014/59/EU genannten nationalen Abwicklungsbehörden, der EZB, dem Einheitlichen Abwicklungsausschuss (bei Informationen über Unternehmen, die in den Geltungsbereich der Verordnung (EU) Nr. 806/2014 fallen), dem ESRB und der ENISA Mechanismen für den Austausch wirksamer Verfahren zwischen Finanzsektoren einrichten, um die Lageerfassung zu verbessern und sektorübergreifend gemeinsame Cyberanfälligkeiten und -risiken zu ermitteln.

Ebenso können sie Krisenmanagement- und Notfallübungen mit Szenarien für Cyberangriffe konzipieren, um Kommunikationskanäle zu entwickeln und schrittweise eine wirksame koordinierte Reaktion auf Unionsebene zu ermöglichen, sofern es zu einem schwerwiegenden grenzüberschreitenden IKT-bezogenen Vorfall oder einer vergleichbaren Bedrohung kommt, die systemische Auswirkungen auf den gesamten Finanzsektor der Union mit sich bringen.

Mit diesen Übungen können gegebenenfalls auch Abhängigkeiten des Finanzsektors von anderen Wirtschaftssektoren untersucht werden.

(2) Die zuständigen Behörden, die ESA und die EZB arbeiten eng zusammen und tauschen Informationen aus, um ihren Aufgaben gemäß den Artikeln 47 bis 54 nachzukommen. Dabei stimmen sie ihre Beaufsichtigungstätigkeit eng untereinander ab, um Verstöße gegen diese Verordnung festzustellen und ihnen entgegenzuwirken, bewährte Verfahren zu entwickeln und zu fördern, die Zusammenarbeit zu erleichtern, eine kohärente Auslegung zu fördern und bei Uneinigkeit eine Bewertung vorzunehmen, die sich nicht nur auf eine einzelne Rechtsordnung stützt.

Artikel 50

Verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen

(1) Die zuständigen Behörden verfügen über alle Aufsichts-, Untersuchungs- und Sanktionsbefugnisse, die zur Erfüllung ihrer Aufgaben im Rahmen dieser Verordnung erforderlich sind.

(2) Die Befugnisse gemäß Absatz 1 umfassen zumindest folgende Befugnisse:

a) den Zugriff auf Unterlagen oder Daten jeglicher Form, die nach Ansicht der zuständigen Behörde für die Ausführung ihrer Aufgaben von Belang sind, sowie den Erhalt oder Anfertigung von Kopien von ihnen;

b) Durchführung von Vor-Ort-Inspektionen oder Untersuchungen, einschließlich unter anderem

   i) der Vorladung von Vertretern der Finanzunternehmen, damit diese mündliche oder schriftliche Erklärungen zu Sachverhalten oder Unterlagen abgeben, die mit Gegenstand und Zweck der Untersuchung in Zusammenhang stehen, sowie der Aufzeichnung der Antworten,

   ii) der Befragung jeder anderen natürlichen oder juristischen Person, die dieser Befragung zum Zweck der Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt;

c) das Verlangen von Korrektur- und Abhilfemaßnahmen bei Verstößen gegen die Anforderungen dieser Verordnung.

(3) Unbeschadet des Rechts der Mitgliedstaaten, strafrechtliche Sanktionen im Einklang mit Artikel 52 zu verhängen, legen die Mitgliedstaaten angemessene verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen für Verstöße gegen diese Verordnung fest und sorgen für deren wirksame Umsetzung.

Diese Sanktionen und Maßnahmen müssen wirksam, verhältnismäßig und abschreckend sein.

(4) Die Mitgliedstaaten übertragen den zuständigen Behörden die Befugnis, bei Verstößen gegen diese Verordnung mindestens die folgenden verwaltungsrechtlichen Sanktionen bzw. Abhilfemaßnahmen anzuwenden:

a) die Erteilung einer Anweisung, wonach die natürliche oder juristische Person gegen diese Verordnung verstoßendes Verhalten zu unterlassen und von einer Wiederholung abzusehen hat;

b) das Verlangen, dass Praktiken oder Verhaltensweisen, die nach Ansicht der zuständigen Behörde den Bestimmungen dieser Verordnung zuwiderlaufen, vorübergehend oder dauerhaft eingestellt und nicht wiederholt werden;

c) das Ergreifen jeder Art von Maßnahme, auch finanzieller Art, um sicherzustellen, dass Finanzunternehmen weiterhin die rechtlichen Anforderungen erfüllen;

d) das Verlangen — soweit gemäß nationalem Recht zulässig — bereits existierender Aufzeichnungen von Datenübermittlungen im Besitz einer Telekommunikationsgesellschaft, wenn der begründete Verdacht auf einen Verstoß gegen die Verordnung besteht und diese Aufzeichnungen für eine Untersuchung von Verstößen gegen diese Verordnung relevant sein könnten; und

e) die Abgabe öffentlicher Bekanntmachungen, einschließlich öffentlicher Bekanntgaben, in denen die Identität der natürlichen oder juristischen Person und die Art des Verstoßes angegeben sind.

(5) Gelten Absatz 2 Buchstabe c und Absatz 4 für juristische Personen, so statten die Mitgliedstaaten die zuständigen Behörden mit der Befugnis aus, Mitgliedern des Leitungsorgans sowie anderen natürlichen Personen, die nach nationalem Recht für den Verstoß verantwortlich sind, vorbehaltlich der nach nationalem Recht geltenden Bedingungen verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen aufzuerlegen.

(6) Die Mitgliedstaaten stellen sicher, dass alle Entscheidungen zur Auferlegung der in Absatz 2 Buchstabe c festgelegten verwaltungsrechtlichen Sanktionen oder Abhilfemaßnahmen ordnungsgemäß begründet werden und dass gegen sie ein Rechtsbehelf eingelegt werden kann.

Artikel 51

Ausübung der Befugnis zur Auferlegung von verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen

(1) Die zuständigen Behörden üben die Befugnisse zur Auferlegung der in Artikel 50 genannten verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen innerhalb ihres nationalen Rechtsrahmens je nach Sachlage in folgender Weise aus:

a) direkt;

b) in Zusammenarbeit mit anderen Behörden;

c) unter ihrer Verantwortung durch Übertragung an andere Behörden oder

d) durch Antragstellung bei den zuständigen Justizbehörden.

(2) Bei der Festlegung von Art und Umfang einer nach Artikel 50 auferlegten verwaltungsrechtlichen Sanktion oder Abhilfemaßnahme berücksichtigen die zuständigen Behörden, inwieweit der Verstoß vorsätzlich erfolgte oder das Ergebnis von Fahrlässigkeit ist, sowie alle anderen relevanten Umstände, darunter auch je nach Sachlage:

a) die Wesentlichkeit, Schwere und Dauer des Verstoßes;

b) der Grad an Verantwortung der für den Verstoß verantwortlichen natürlichen oder juristischen Person;

c) die Finanzkraft der verantwortlichen natürlichen oder juristischen Person;

d) die Höhe der von der verantwortlichen natürlichen oder juristischen Person erzielten Gewinne oder verhinderten Verluste, sofern sich diese beziffern lassen;

e) die Verluste, die Dritten durch den Verstoß entstanden sind, sofern sich diese beziffern lassen;

f) die Bereitschaft der verantwortlichen natürlichen oder juristischen Person zur Zusammenarbeit mit der zuständigen Behörde, unbeschadet des Erfordernisses, die von dieser natürlichen oder juristischen Person erzielten Gewinne oder verhinderten Verluste einzuziehen;

g) frühere Verstöße der verantwortlichen natürlichen oder juristischen Person.

Artikel 52

Strafrechtliche Sanktionen

(1) Mitgliedstaaten können beschließen, für Verstöße, die nach ihrem nationalen Recht strafrechtlichen Sanktionen unterliegen, keine Vorschriften für verwaltungsrechtliche Sanktionen oder Abhilfemaßnahmen festzulegen.

(2) Mitgliedstaaten, die strafrechtliche Sanktionen für die in dieser Verordnung genannten Verstöße festgelegt haben, stellen durch angemessene Maßnahmen sicher, dass die zuständigen Behörden über alle notwendigen Befugnisse verfügen, um sich mit den Justiz-, Strafverfolgungs- oder Strafjustizbehörden in ihrem Hoheitsgebiet ins Benehmen zu setzen, um spezifische Informationen im Zusammenhang mit strafrechtlichen Ermittlungen oder Verfahren, die wegen der Verstöße gegen diese Verordnung eingeleitet wurden, zu erhalten und diese anderen zuständigen Behörden sowie der EBA, der ESMA oder der EIOPA zur Verfügung zu stellen, um ihre Pflichten zur Zusammenarbeit für die Zwecke dieser Verordnung zu erfüllen.

Artikel 53

Mitteilungspflichten

Die Mitgliedstaaten teilen der Kommission, der ESMA, der EBA und der EIOPA bis zum 17. Januar 2025 die Gesetze, sonstige Vorschriften sowie Verwaltungsvorschriften, einschließlich der einschlägigen strafrechtlichen Vorschriften, zur Umsetzung dieses Kapitels mit. Die Mitgliedstaaten teilen der Kommission, der ESMA, der EBA und der EIOPA spätere Änderungen dieser Vorschriften unverzüglich mit.

Artikel 54

Öffentliche Bekanntmachung verwaltungsrechtlicher Sanktionen

(1) Die zuständigen Behörden veröffentlichen auf ihren amtlichen Websites unverzüglich jede Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion, gegen die nach Mitteilung dieser Entscheidung an die Person, gegen die die Sanktion verhängt wurde, kein Rechtsbehelf eingelegt werden kann.

(2) Die in Absatz 1 genannte Bekanntmachung umfasst Informationen zu Art und Natur des Verstoßes, der Identität der verantwortlichen Personen und der verhängten Sanktionen.

(3) Gelangt die zuständige Behörde nach einer Einzelfallprüfung zu der Auffassung, dass die Bekanntmachung der Identität im Falle juristischer Personen oder der Identität und der personenbezogenen Daten im Falle natürlicher Personen unverhältnismäßig wäre, was auch Risiken für den Schutz personenbezogener Daten einschließt, die Stabilität der Finanzmärkte oder die Durchführung laufender strafrechtlicher Ermittlungen gefährden oder der betroffenen Person einen unverhältnismäßigen Schaden zufügen würde — soweit dieser ermittelt werden kann —, so beschließt sie in Bezug auf die Entscheidung, mit der eine verwaltungsrechtliche Sanktion verhängt wird, eine der folgenden Lösungen:

a) Aufschub der Veröffentlichung bis alle Gründe für die Nichtveröffentlichung wegfallen;

b) anonyme Veröffentlichung im Einklang mit dem nationalen Recht; oder

c) Unterlassung der Veröffentlichung, wenn die unter den Buchstaben a und b genannten Optionen entweder nicht ausreichen, um zu gewährleisten, dass keine Gefahr für die Stabilität der Finanzmärkte besteht, oder wenn eine solche Veröffentlichung nicht mit der bei der Verhängung der Sanktion angewandten Nachsicht vereinbar wäre.

(4) Wird entschieden, eine verwaltungsrechtliche Sanktion gemäß Absatz 3 Buchstabe b in anonymisierter Form bekannt zu machen, so kann die Bekanntmachung der einschlägigen Angaben aufgeschoben werden.

(5) Macht eine zuständige Behörde eine Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion, gegen die ein Rechtsbehelf bei den einschlägigen Justizbehörden eingelegt worden ist, bekannt, so fügen die zuständigen Behörden diese Information ihrer amtlichen Website unverzüglich und etwaige nachfolgende Informationen über den Ausgang des Rechtsbehelfsverfahrens zu einem späteren Zeitpunkt hinzu. Gerichtliche Entscheidungen, mit denen eine Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion für nichtig erklärt wird, werden ebenfalls bekannt gemacht.

(6) Die zuständigen Behörden stellen sicher, dass die in den Absätzen 1 bis 4 genannten Bekanntmachungen nur so lange auf ihrer amtlichen Website verbleiben, wie es zum Zwecke dieses Artikels erforderlich ist. Dieser Zeitraum darf fünf Jahre ab dem Zeitpunkt der Veröffentlichung nicht überschreiten.

Artikel 55

Wahrung des Berufsgeheimnisses

(1) Vertrauliche Informationen, die gemäß dieser Verordnung empfangen, ausgetauscht oder übermittelt werden, unterliegen den in Absatz 2 festgelegten Bestimmungen zum Berufsgeheimnis.

(2) Zur Wahrung des Berufsgeheimnisses verpflichtet sind alle Personen, die bei den gemäß dieser Verordnung zuständigen Behörden oder bei einer Behörde, einem Marktteilnehmer oder einer natürlichen oder juristischen Person beschäftigt sind oder waren, an die bzw. den diese zuständigen Behörden ihre Befugnisse delegiert haben, einschließlich unter Vertrag genommener Revisoren und Sachverständigen.

(3) Unter das Berufsgeheimnis fallende Informationen, einschließlich der zwischen den gemäß der vorliegenden Verordnung zuständigen Behörden und den gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden ausgetauschten Informationen, dürfen keiner anderen Person oder Behörde gegenüber offengelegt werden, es sei denn, dies geschieht aufgrund von Unionsrecht oder nationalem Recht.

(4) Alle gemäß dieser Verordnung zwischen den zuständigen Behörden ausgetauschten Informationen, die Geschäfts- oder Betriebsbedingungen und andere wirtschaftliche oder persönliche Angelegenheiten betreffen, werden als vertraulich betrachtet und unterliegen den Anforderungen an das Berufsgeheimnis, es sein denn, ihre Weitergabe wird von der zuständigen Behörde zum Zeitpunkt der Mitteilung für zulässig erklärt oder ist für Gerichtsverfahren erforderlich.

Artikel 56

Datenschutz

(1) Die ESA und die zuständigen Behörden dürfen personenbezogene Daten nur verarbeiten, wenn dies zur Erfüllung ihrer jeweiligen Pflichten und Aufgaben gemäß dieser Verordnung erforderlich ist, insbesondere für Untersuchungen, Inspektionen, Auskunftsersuchen, Kommunikationszwecke, Veröffentlichungen, Evaluierungen, Verifizierungen, Bewertungen und die Erstellung von Überwachungsplänen. Die personenbezogenen Daten müssen im Einklang mit der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 verarbeitet werden, je nachdem, welche der beiden anwendbar ist.

(2) Sofern in anderen sektorspezifischen Rechtsakten nichts anderes vorgesehen ist, werden die in Absatz 1 genannten personenbezogenen Daten bis zur Erfüllung der geltenden Aufsichtspflichten, in jedem Fall aber für höchstens 15 Jahre aufbewahrt, außer bei anhängigen Gerichtsverfahren, die eine weitere Speicherung dieser Daten erfordern.

KAPITEL VIII

Delegierte Rechtsakte

Artikel 57

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 17. Januar 2024 übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(3) Die Befugnisübertragung gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen, im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

KAPITEL IX

Übergangs- und Schlussbestimmungen

Abschnitt I

Artikel 58

Überprüfungsklausel

(1) Bis zum 17. Januar 2028 führt die Kommission nach Konsultation der ESA und des ESRB, je nach Sachlage, eine Überprüfung durch und legt dem Europäischen Parlament und dem Rat einen Bericht vor, gegebenenfalls zusammen mit einem Gesetzgebungsvorschlag. Die Überprüfung muss sich mindestens auf Folgendes erstrecken:

a) die Kriterien für die Benennung kritischer IKT-Drittdienstleister gemäß Artikel 31 Absatz 2;

b) die Freiwilligkeit der Meldung erheblicher Cyberbedrohungen gemäß Artikel 19;

c) die Regelung gemäß Artikel 31 Absatz 12 und die Befugnisse der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d Ziffer iv erster Gedankenstrich, um die Wirksamkeit dieser Bestimmungen im Hinblick auf die Gewährleistung einer wirksamen Überwachung kritischer IKT-Drittdienstleister mit Sitz in einem Drittland und die Notwendigkeit der Gründung eines Tochterunternehmens in der Union zu bewerten.

   Für die Zwecke von Unterabsatz 1 dieses Buchstabens umfasst die Überprüfung eine Analyse der Regelung gemäß Artikel 31 Absatz 12, einschließlich hinsichtlich der Bedingungen für den Zugang von Finanzunternehmen der Union zu Dienstleistungen aus Drittländern und der Verfügbarkeit dieser Dienstleistungen auf dem Unionsmarkt, und berücksichtigt weitere Entwicklungen auf den Märkten für die unter diese Verordnung fallenden Dienstleistungen, die von Finanzunternehmen und Finanzaufsichtsbehörden bei der Anwendung dieser Regelung bzw. der damit verbundenen Beaufsichtigung gewonnenen praktischen Erfahrungen sowie alle einschlägigen regulatorischen und aufsichtlichen Entwicklungen auf internationaler Ebene.

d) die Angemessenheit der Einbeziehung derjenigen in Artikel 2 Absatz 3 Buchstabe e genannten Finanzunternehmen in den Geltungsbereich dieser Verordnung, die automatisierte Vertriebssysteme nutzen, unter Berücksichtigung künftiger Marktentwicklungen im Zusammenhang mit der Nutzung solcher Systeme;

e) die Funktionsweise und Wirksamkeit des JON bei der Förderung der Kohärenz der Überwachung und der Effizienz des Informationsaustauschs innerhalb des Überwachungsrahmens.

(2) Im Zusammenhang mit der Überprüfung der Richtlinie (EU) 2015/2366 bewertet die Kommission, ob die Resilienz von Zahlungssystemen und Zahlungsabwicklungstätigkeiten gegenüber Cyberangriffen erhöht werden muss und ob es angemessen ist, den Geltungsbereich dieser Verordnung auf Betreiber von Zahlungssystemen und an Zahlungsabwicklungstätigkeiten beteiligte Stellen auszuweiten. Die Kommission legt unter Berücksichtigung des Ergebnisses dieser Bewertung dem Europäischen Parlament und dem Rat im Rahmen der Überprüfung der Richtlinie (EU) 2015/2366 bis spätestens 17. Juli 2023 einen Bericht vor.

Auf der Grundlage dieses Überprüfungsberichts und nach Konsultation der ESA, der EZB und des ESRB kann die Kommission gegebenenfalls als Teil des Gesetzgebungsvorschlags, den sie gemäß Artikel 108 Unterabsatz 2 der Richtlinie (EU) 2015/2366 annehmen kann, einen Vorschlag unterbreiten, mit dem sichergestellt wird, dass alle Betreiber von Zahlungssystemen und alle an Zahlungsabwicklungstätigkeiten beteiligte Stellen einer angemessenen Überwachung unterliegen, wobei der bestehenden Überwachung durch die Zentralbank Rechnung zu tragen ist.

(3) Bis zum 17. Januar 2026 führt die Kommission nach Konsultation der ESA und des Ausschusses der Europäischen Aufsichtsstellen für Abschlussprüfer eine Überprüfung durch und legt — gegebenenfalls zusammen mit einem Gesetzgebungsvorschlag — dem Europäischen Parlament und dem Rat einen Bericht darüber vor, ob strengere Anforderungen an Abschlussprüfer und Prüfungsgesellschaften in Bezug auf die digitale operationale Resilienz angemessen sind, indem Abschlussprüfer und Prüfungsgesellschaften in den Geltungsbereich der vorliegenden Verordnung aufgenommen werden oder die Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates ([39]) geändert wird.

Abschnitt II

Änderungen

Artikel 59

Änderungen der Verordnung (EG) Nr. 1060/2009

Die Verordnung (EG) Nr. 1060/2009 wird wie folgt geändert:

1. Anhang I Abschnitt A Nummer 4 Unterabsatz 1 erhält folgende Fassung:

„Eine Ratingagentur verfügt über eine solide Verwaltung und Rechnungslegung, interne Kontrollmechanismen, effiziente Verfahren für die Risikobewertung sowie wirksame Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

(*) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).“

2. Anhang III Nummer 12 erhält folgende Fassung:

„12. Die Ratingagentur verstößt gegen Artikel 6 Absatz 2 in Verbindung mit Anhang I Abschnitt A Nummer 4, wenn sie über keine solide Verwaltung und Rechnungslegung, keine internen Kontrollmechanismen, keine effizienten Verfahren für die Risikobewertung oder keine wirksamen Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 verfügt oder wenn sie keine Entscheidungsprozesse oder keine Organisationsstruktur nach Maßgabe jener Nummer schafft oder unterhält.“

Artikel 60

Änderungen der Verordnung (EU) Nr. 648/2012

Die Verordnung (EU) Nr. 648/2012 wird wie folgt geändert:

1. Artikel 26 wird wie folgt geändert:

a) Absatz 3 erhält folgende Fassung:

„(3) Eine CCP muss dauerhaft über eine Organisationsstruktur verfügen, die Kontinuität und ein ordnungsgemäßes Funktionieren im Hinblick auf die Erbringung ihrer Dienstleistungen und Ausübung ihrer Tätigkeiten gewährleistet. Sie muss angemessene und verhältnismäßige Systeme, Ressourcen und Verfahren einsetzen, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) betrieben werden.

(*) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).“

([39]) Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates (ABl. L 157 vom 9.6.2006, S. 87).

b) Absatz 6 wird gestrichen;

2. Artikel 34 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Eine CCP hat eine angemessene Geschäftsfortführungsleitlinie sowie einen Notfallwiederherstellungsplan — der eine IKT-Geschäftsfortführungsleitlinie und IKT- Reaktions- und Wiederherstellungspläne umfasst, die nach der Verordnung (EU) 2022/2554 aufgestellt und umgesetzt werden — festzulegen, umzusetzen und zu befolgen, mit dem Ziel eine Aufrechterhaltung der Funktionen der CCP, eine rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie eine Erfüllung der Pflichten der CCP zu gewährleisten."

b) Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) Um die einheitliche Anwendung dieses Artikels zu gewährleisten, erarbeitet die ESMA nach Anhörung der Mitglieder des ESZB Entwürfe für technische Regulierungsstandards, in denen der Mindestinhalt und die Anforderungen an die Geschäftsfortführungsleitlinie und an den Notfallwiederherstellungsplan, unter Ausschluss der IKT-Geschäftsfortführungsleitlinie und der Pläne für Notfallwiederherstellung, festgelegt werden."

3. Artikel 56 Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) Um die einheitliche Anwendung dieses Artikels zu gewährleisten, erarbeitet die ESMA Entwürfe für technische Regulierungsstandards, in denen die Einzelheiten des in Absatz 1 genannten Antrags auf Registrierung festgelegt werden, mit Ausnahme der Anforderungen im Zusammenhang mit dem IKT-Risikomanagement."

4. Artikel 79 Absätze 1 und 2 erhält folgende Fassung:

„(1) Ein Transaktionsregister ermittelt Quellen operationeller Risiken und minimiert diese Risiken durch die Entwicklung angemessener Systeme, Kontrollen und Verfahren, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 betrieben werden.

(2) Ein Transaktionsregister hat eine angemessene Geschäftsfortführungsleitlinie und einen Notfallwiederherstellungsplan — einschließlich einer IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungsplänen, die nach der Verordnung (EU) 2022/2554 eingerichtet werden — festzulegen, umzusetzen und zu befolgen, mit dem Ziel, die Aufrechterhaltung der Funktionen des Transaktionsregisters, die rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie die Erfüllung der Pflichten des Transaktionsregisters zu gewährleisten."

5. Artikel 80 Absatz 1 wird gestrichen;

6. Anhang I Abschnitt II wird wie folgt geändert:

a) Die Buchstaben a und b erhalten folgende Fassung:

„a) Ein Transaktionsregister verstößt gegen Artikel 79 Absatz 1, wenn es nicht die Quellen betrieblicher Risiken ermittelt bzw. diese Risiken nicht durch die Entwicklung angemessener Systeme, Kontrollen und Verfahren, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 betrieben werden, minimiert.

b) Ein Transaktionsregister verstößt gegen Artikel 79 Absatz 2, wenn es nicht eine angemessene Geschäftsfortführungsleitlinie und einen Notfallwiederherstellungsplan, die nach der Verordnung (EU) 2022/2554 eingerichtet werden, festlegt, umsetzt oder aufrechterhält, mit dem Ziel, die Aufrechterhaltung der Funktionen des Transaktionsregisters, die zeitnahe Wiederherstellung des Geschäftsbetriebs sowie die Erfüllung der Pflichten des Transaktionsregisters zu gewährleisten."

b) Buchstabe c wird gestrichen;

7. Anhang III wird wie folgt geändert:

a) Abschnitt II wird wie folgt geändert:

i) Buchstabe c erhält folgende Fassung:

„c) eine Tier 2-CCP verstößt gegen Artikel 26 Absatz 3, wenn sie nicht dauerhaft über eine Organisationsstruktur verfügt, die Kontinuität und ein ordnungsgemäßes Funktionieren im Hinblick auf die Erbringung ihrer Dienstleistungen und Ausübung ihrer Tätigkeiten gewährleistet, oder wenn sie keine angemessenen und geeigneten Systeme, Ressourcen und Verfahren einsetzt, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 (DORA) betrieben werden;"

ii) Buchstabe f wird gestrichen.

b) in Abschnitt III erhält Buchstabe a folgende Fassung:

„a) eine Tier 2-CCP verstößt gegen Artikel 34 Absatz 1, wenn sie keine angemessene Geschäftsfortführungsleitlinie und keinen Reaktions- und Wiederherstellungsplan, die nach der Verordnung (EU) 2022/2554 eingerichtet werden, festlegt, umsetzt und befolgt, mit dem Ziel, eine Aufrechterhaltung der Funktionen der CCP, eine rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie eine Erfüllung der Pflichten der CCP zu gewährleisten, wobei ein solcher Plan zumindest eine Wiederherstellung aller Transaktionen zum Zeitpunkt der Störung ermöglichen muss, sodass die CCP weiterhin zuverlässig arbeiten und die Abwicklung zum geplanten Termin vornehmen kann;“

Artikel 61

Änderungen der Verordnung (EU) Nr. 909/2014

Artikel 45 der Verordnung (EU) Nr. 909/2014 wird wie folgt geändert:

1. Absatz 1 erhält folgende Fassung:

„(1) Ein Zentralverwahrer ermittelt Quellen des internen und externen operationellen Risikos und hält deren Auswirkungen durch den Einsatz angemessener IKT-Tools, Verfahren und Strategien, die gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichtet und verwaltet werden, sowie durch alle anderen relevanten angemessenen Instrumente, Kontrollen und Verfahren für andere Arten operationeller Risiken, auch für alle von ihm betriebenen Wertpapierliefer- und -abrechnungssysteme, so gering wie möglich.

_____

(*) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1).“

2. Absatz 2 wird gestrichen;

3. Absätze 3 und 4 erhalten folgende Fassung:

„(3) Für die von ihm erbrachten Dienstleistungen und jedes von ihm betriebene Wertpapierliefer- und -abrechnungssystem legt ein Zentralverwahrer eine angemessene Geschäftsfortführungsleitlinie sowie einen Notfallwiederherstellungsplan, einschließlich einer IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungspläne, die gemäß der Verordnung (EU) 2022/2554 eingerichtet werden, fest, die er anwendet und befolgt, um bei Ereignissen, die ein beträchtliches Risiko einer Beeinträchtigung des Geschäftsbetriebs bergen, das Aufrechterhalten der Dienstleistungen, die rasche Wiederherstellung des Geschäftsbetriebs und die Erfüllung seiner Pflichten zu gewährleisten.

(4) Der Plan nach Absatz 3 muss eine Wiederherstellung aller Geschäfte und Positionen der Teilnehmer zum Zeitpunkt der Störung ermöglichen, damit die Teilnehmer eines Zentralverwahrers ihre Tätigkeiten in sicherer Weise fortsetzen und Lieferungen und Abrechnungen zum geplanten Termin vornehmen können; hierzu gehört auch die Vorsorge, dass kritische IT-Systeme nach der Störung wieder in Betrieb genommen werden können, so wie in Artikel 12 Absätze 5 und 7 der Verordnung (EU) 2022/2554 vorgesehen.“

4. Absatz 6 erhält folgende Fassung:

„(6) Ein Zentralverwahrer ermittelt, überwacht und managt die Risiken, die von wichtigen Teilnehmern an den von ihm betriebenen Wertpapierliefer- und -abrechnungssystemen sowie von Dienstleistern und Versorgungsbetrieben, anderen Zentralverwahrern oder anderen Marktinfrastrukturen für seinen Geschäftsbetrieb ausgehen könnten. Er unterrichtet die zuständige Behörde sowie die betreffenden Behörden auf Verlangen über alle solchermaßen ermittelten Risiken. Er unterrichtet die zuständige Behörde sowie die betreffenden Behörden ferner unverzüglich über alle Störfälle infolge dieser Risiken, die nicht im Zusammenhang mit dem IKT-Risiko auftreten.“

5. Absatz 7 Unterabsatz 1 erhält folgende Fassung:

„(7) Die ESMA arbeitet in enger Abstimmung mit den Mitgliedern des ESZB Entwürfe technischer Regulierungsstandards aus, in denen die operationellen Risiken nach den Absätzen 1 und 6 — mit Ausnahme von IKT-Risiken — sowie die Verfahren zur Prüfung, Bewältigung oder Minimierung dieser Risiken einschließlich der Geschäftsfortführungsleitlinien und der Notfallsanierungspläne nach den Absätzen 3 und 4 sowie der Verfahren zu ihrer Beurteilung präzisiert werden.“

Artikel 62

Änderungen der Verordnung (EU) Nr. 600/2014

Die Verordnung (EU) Nr. 600/2014 wird wie folgt geändert:

1. Artikel 27g wird wie folgt geändert:

   a) Absatz 4 erhält folgende Fassung:

   „(4) Ein APA muss die in der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   _____

   (*) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1)."

   b) Absatz 8 Buchstabe c erhält folgende Fassung:

   „c) die konkreten organisatorischen Anforderungen nach den Absätzen 3 und 5."

2. Artikel 27h wird wie folgt geändert:

   a) Absatz 5 erhält folgende Fassung:

   „(5) Ein CTP muss die in der Verordnung (EU) 2022/2554 festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   b) in Absatz 8 erhält Buchstabe e folgende Fassung:

   „e) die konkreten organisatorischen Anforderungen nach Absatz 4."

3. Artikel 27i wird wie folgt geändert:

   a) Absatz 3 erhält folgende Fassung:

   „(3) Ein ARM muss die in der Verordnung (EU) 2022/2554 festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   b) Absatz 5 Buchstabe b erhält folgende Fassung:

   „b) die konkreten organisatorischen Anforderungen nach den Absätzen 2 und 4."

Artikel 63

Änderungen der Verordnung (EU) 2016/1011

In Artikel 6 der Verordnung (EU) 2016/1011 wird folgender Absatz angefügt:

„(6) Für kritische Referenzwerte verfügt ein Administrator über eine solide Verwaltung und Rechnungslegung, interne Kontrollmechanismen, effiziente Verfahren für die Risikobewertung sowie wirksame Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

_____

(*) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1)."

Artikel 64

Inkrafttreten und Anwendung

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 17. Januar 2025.

Diese Verordnung ist in allen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Straßburg am 14. Dezember 2022.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	M. BEK